

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: January 21, 2010

Name of company covered by this certification: Go Solo Technologies, Inc.

Form 499 Filer ID: 822790

Name of signatory: Michael A. Richard

Title of signatory: Treasurer

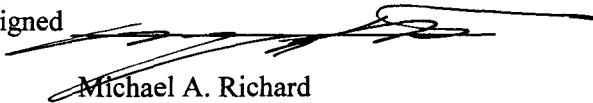
I, Michael A. Richard, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules at 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. The Company has no information with respect to the processes pretexters are using to attempt to access CPNI, or what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



Michael A. Richard

Go Solo Technologies Procedures for Disclosure of CPNI

Go Solo Technologies is committed to maintaining the privacy of its customers and protecting their CPNI and other all other customer data. The procedures we follow are set out below.

WHAT IS PROTECTED

Go Solo Technologies has a duty, under federal law, to protect the confidentiality of certain types of customer proprietary network information (CPNI), including: (1) information about the quantity, technical configuration, type, destination, location, and amount of use of a Customer's services, and (2) information contained on the service bill concerning services a Customer receives. CPNI includes information typically available from the telephone-related details on a monthly bill, such as technical information, type of service, current charges, long distance and local service billing records, directory assistance charges, usage data and calling patterns.

HOW IT IS PROTECTED

Go Solo Technologies does not use third party marketing organizations. However, Go Solo Technologies does have a contract with a professional employee organization, Strategic Outsourcing, Inc. ("SOI"), that governs all of Go Solo Technologies' staff members. All of Go Solo Technologies' staff, are technically employees of SOI. Under the SOI contract, Go Solo Technologies has the right to determine the employment and workplace rules and policies applicable to the SOI employees assigned to Go Solo Technologies. Go Solo requires all such assigned employees ("staff members") to protect the confidential information of Go Solo Technologies, including the CPNI of its customers. Strategic Outsourcing itself has no access to CPNI in the possession of Go Solo Technologies.

Go Solo Technologies' protection of CPNI begins with training. All our staff members are trained on how CPNI is to be protected and when it may or may not be disclosed. Violation of this CPNI policy by any staff member will result in disciplinary action against that staff member.

Go Solo Technologies has different procedures in place depending on the method by which a party seeks access to CPNI.

Initial Verification

Go Solo Technologies authenticates each customer's identity and requires him or her to select a password upon service initiation. We do not use readily available personal information or account information in setting up the procedure for subsequent authentication for purposes of making account changes or allowing the customer access to CPNI related to his or her account. Once the customer's identity is initially

authenticated, the customer may only obtain access to his or her CPNI online, through use of a password.

No Telephone Access to CPNI

Go Solo Technologies has a strict policy and will not release CPNI over the telephone during customer-initiated telephone contact.

Internet Access

To get access to information such as call detail records and other customer proprietary information, all customers must log into their account over the Internet. They must use their telephone number of record and their designated password.

Lost or Forgotten Passwords

In the event a customer has lost or forgotten a password, he must contact Go Solo Technologies and we use the information selected at account initiation – which is neither readily available personal information nor account information – to verify the caller's identity and request. Only then is the account password sent to the caller via email. The email address used is the one already on record, which was obtained from the customer upon service initiation.

Notification of Account Changes

Go Solo Technologies notifies its customers immediately whenever there is CPNI-related account activity, such as a password change, a customer inquiring for a lost or forgotten password, the creation of a new online account, or the change of the address of record. The first notification, including the selection of a password at service initiation, is sent to the customer upon activation of service. Subsequent notifications are sent to the customer at the then-current email address of record, and do not reveal the changed information.

Business and Wholesale Customers

In dealing with business and wholesale customers, Go Solo Technologies ordinarily contracts for authentication regimes other than those described in Sections 64.2010 and 64.2011 of the FCC rules because it provides those customers with a dedicated account representative and it enters into a contract that specifically addresses its and the customer's protection of CPNI.

BREACH OF CPNI PRIVACY

In the event Go Solo Technologies experiences a privacy breach and CPNI is disclosed to unauthorized persons, federal rules require Go Solo Technologies to report such breaches

to the U.S. Secret Service and the FBI. Any Go Solo Technologies staff member learning of such a breach must notify senior management immediately. Go Solo Technologies will notify law enforcement no later than seven (7) business days after it has reasonably determined that such breach has occurred by sending electronic notification to the United States Secret Service and the FBI through the central reporting facility at www.fcc.gov/eb/cpni.

No staff member shall notify any customer of a breach without written authorization from the president of Go Solo Technologies. By law, Go Solo Technologies cannot inform its customers of the CPNI breach until at least seven (7) days after notification has been sent to law enforcement, or later if the law enforcement agency tells it to postpone disclosure pending investigation.

Go Solo Technologies is required to and will maintain records of any discovered CPNI breaches, the date that it discovered the breach, the date it notified law enforcement and copies of the notifications to law enforcement, a detailed description of the breach, including the circumstances of the breach, and law enforcement's response (if any) to the reported breach. Go Solo Technologies will retain these records for a period of not less than two (2) years.

NOTIFICATION OF CHANGES TO THIS POLICY

If we change this CPNI Policy, we will post those changes to our website or in other places we deem appropriate, so that our customers can be aware of what information we collect, how we use it, and under what circumstances, if any, we disclose it.